EXHIBIT B

U.S. Department of the Treasury

Crypto-Assets:

Implications for Consumers, Investors, and Businesses

September 2022

into popular games, as well as the development of blockchain-native games, means that players can purchase tokenized game features and attributes which they own and are able to transfer.[103] In addition, online or blockchain-enabled "metaverses"—digital worlds where participants can interact virtually with other users and purchase tokenized digital real estate and other "merchandise"—have grown in popularity as form of entertainment. With an estimated 215 million, or 66% of, Americans playing video games at least once per week, the potential market for such so-called "play-to-earn" games is substantial.[104]

Potential Opportunities in NFTs

NFTs have a number of potential future applications, including: (i) enabling the recording and verification of transfers of real estate ownership; (ii) facilitating automatic royalty payments for music and film; (iii) preventing duplication and counterfeits in the titling of other property and consumer goods; (iv) enabling more digital credentials, including identification, licensing, certification; and (v) facilitating financial industry legal compliance.

NFTs have the potential to function across both digital spaces and the physical world. As a result, NFTs can include features that serve as membership cards or tickets, providing access to events, exclusive merchandise, and special discounts.[105] However, many of the potential NFT use cases are still materializing, in part due to evolving technological and legal landscape, including with respect to licensing, contracts, copyright and intellectual property, anti-money laundering, and data protection.[106]

IV. RISKS AND EXPOSURES FOR CONSUMERS, INVESTORS, AND BUSINESSES

Having considered the potential opportunities presented by crypto-asset products and services, this part of the report reviews the risks posed by crypto-assets. These risks are divided into three categories: (i) conduct risks, including product, and investor, consumer, and business protection (e.g., theft, fraud) risks; (ii) operational risks, including the technology-specific risks of crypto-assets and systems; and (iii) risks arising from crypto-asset intermediation. Some of the risks discussed in this part are unique to the crypto-asset ecosystem, as a result of the features of crypto-assets. Others are simply a form of risk already present in traditional finance markets, but which is heightened due to the specific attributes of the crypto-asset ecosystem.

103 Though tokenized game features and attributes are, on the surface, intended to enhance players' experiences within the gaming environment, to the extent these NFTs have tradable value there is a possibility that some players will become incentivized to use them predominantly as speculative assets, purchasing in-game NFTs primarily with the aim of selling them for a future profit. Indeed, players both in the U.S. and abroad have taken to playing certain games as a way to earn a living, and some games have deployed design features and incentives in order to create an "investor mindset" among new players. In addition, the increased prevalence of "gamification" of investment activities more generally has come under greater scrutiny in recent years. *See* James Fallows Tierney, *Investment Games*, Duke Law Journal (Vol. 72, Forthcoming 2022-23), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3916407.

104 Entertainment Software Association, Essential Facts About the Video Game Industry (2022), https://www.theesa.com/resource/2022-essential-facts-about-the-video-game-industry.

105 Steve Kaczynski & Scott Duke Kominers, *How NFTs Create Value*, Harvard Business Review (Nov. 10, 2021), https://hbr.org/2021/11/how-nfts-create-value.

106 For example, since NFTs essentially represent the original and unique cryptographic code or on-chain token linked to the off-chain digital work or real-world asset, ownership of an NFT may not translate to ownership of an underlying asset or the associated rights (such as copyright and licensing rights). *See, e.g.*, Stuart Levi, Mana Ghaemmaghami & Gabriel Mohr, *Skadden Discusses the Growing Complexity of Commercial Rights Issues In NFTs*, The CLS Blue Sky Blog (Jun. 1, 2022), https://clsbluesky.law.columbia.edu/2022/06/01/skadden-discusses-the-growing-complexity-of-commercial-rights-issues-in-nfts. NFTs can also be used to facilitate money laundering and terror financing; digital art assets are inherently easier than traditional art for such purposes. *See* U.S. Department of the Treasury, Study of the Facilitation of Money Laundering and Terror Finance Through The Trade in the Works of Art (2022), https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf.

This part then considers factors affecting the relative exposure of consumers, investors, and businesses to these risks, including due to market participants' non-compliance with current laws and regulations, and ongoing changes related to the scope and application of those legal requirements.

Conduct Risks

Consumers, investors, and businesses using or investing in crypto-assets are exposed to a variety of conduct risks in the crypto-asset ecosystem. Investing is often at the core of crypto-asset activity; accordingly, the conduct risks below largely focus on risks associated with investing activities.

Crypto-assets and markets that operate out of compliance with applicable laws and regulations, or are unregulated, can breed fraud, abusive market practices, and disclosure gaps.[107] Certain practices in the crypto-asset ecosystem have resulted in financial harm to consumers, investors, and businesses; unfair and inequitable outcomes; and damage to the integrity of the market. Some notable conduct risks are described below, but risks are likely to continue to evolve as crypto-asset markets change and therefore require vigilant and robust regulatory supervision and oversight.[108]

Fraud, Theft, and Mismanagement

As the crypto-asset market has grown, so has the volume of fraud, scams, and theft in the ecosystem; indeed, unlawful transaction activity globally reached an all-time high in value in 2021.[109]

Criminals often take advantage of innovations and new technologies to perpetrate fraudulent activities, including promises or guarantees of high returns. Moreover, the crypto-asset ecosystem has unique features that make it an increasingly attractive target for unlawful activity, including the ongoing evolution of the underlying technology, pseudonymity, irreversibility of transactions, and the current asymmetry of information between issuers of crypto-assets and consumers and investors.

Multiple U.S. government agencies track and publish crypto-asset related complaints reported by the public, which have indicated a sharp increase in losses related to crypto-assets. They have also issued warnings related to their findings, including noting a material increase in crypto-assets as a payment method for all types of scams, including investment scams, romance scams, and business and government impersonation scams.[110]

- The Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) has warned against the scams leveraging cryptocurrency ATMs,[111] cryptocurrency customer support impersonators, as well as romance scams that involve investment opportunities. In 2021, the IC3 received 34,202

107 IOSCO, *supra* note 21, at 36.

108 *Id.*, at 5.

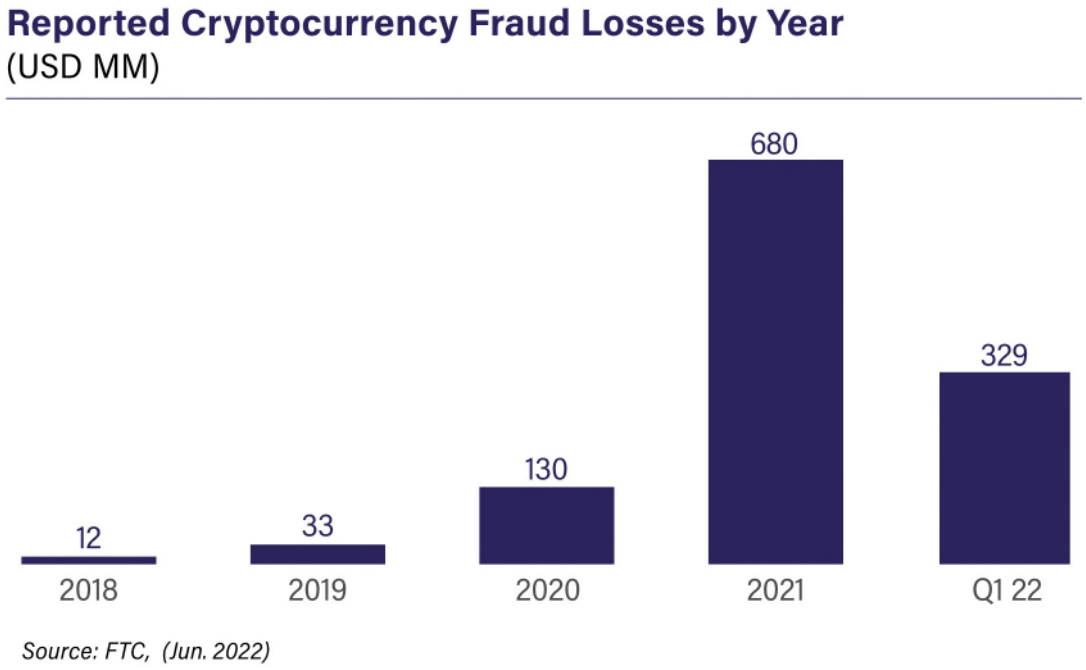
109 At the same time, transaction activity associated with unlawful applications reached an all-time low as a share of all crypto-asset activity, reflecting the growth in overall transaction volume. *See* Chainalysis, The 2022 Crypto Crime Report 3-4 (2022), https://go.chainalysis.com/2022-Crypto-Crime-Report.html.

110 For more information on crypto-asset scams, see FTC, *Reports show scammers cashing in on crypto craze*, (Jun. 2022), www.ftc.gov/system/files/ftc_gov/pdf/Crypto%20Spotlight%20FINAL%20June%202022.pdf.

111 Criminal actors, in various fraudulent schemes, maliciously leverage physical cryptocurrency ATMs to receive payments from victims. *See, e.g.*, FBI, T*he FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment*, (Nov. 4, 2021), https://www.ic3.gov/Media/Y2021/PSA211104.

complaints involving the use of some type of crypto-asset. While the number of complaints decreased by approximately 3% in 2021 year-over-year, the loss amount reported in IC3 complaints increased by nearly 600%, from $246 million in 2020 to more than $1.6 billion in 2021.[112]

- The Consumer Financial Protection Bureau (CFPB) had 2,404 published crypto-asset consumer complaints in 2021 compared to 983 in 2020, amounting an increase of over 140%. As of July 15, 2022, the CFPB had 906 complaints year-to-date and 1,870 published complaints in the prior 12 months.[113]
- The Federal Trade Commission (FTC) had more than 46,000 reported incidents of fraud between January 1, 2021, and March 31, 2022, with people claiming losses that exceeded $1 billion worth of cryptocurrencies. Cryptocurrencies represented 24% of all fraud-related losses reported to the FTC during that period—more than any other payment method.[114] The median individual reported loss was $2,600.[115]



Measuring or estimating the volume of crime involving crypto-assets, or any criminal activity, can be challenging as it relies on self-reporting by victims and thus is likely to be underreported. However, given the public nature of blockchains, several private firms have been able to use proprietary methodologies to track losses from known thefts, scams, and frauds. According to one private sector estimate, there was $14 billion worth of crypto-asset-based crime, globally, in 2021, up from $7.8 billion in 2020; the breakdown is as follows:

- *Scams:* Scams were the largest form of crypto-asset-based crime by transaction volume in 2021. The number of scams in 2021 rose by over 60% year-over-year, while the value of stolen crypto-

112 FBI, 2021 Internet Crime Report 13 (2021), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

113 CFPB, *CFPB Complaint Database*, https://www.consumerfinance.gov/data-research/consumer-complaints/search.

114 FTC, *supra* note 110.

115 *Id.*

assets rose by over 80% in 2021 to $7.8 billion. $2.8 billion of this total came from a relatively new but increasingly common scheme known as a "rug pull," in which developers build out what appears to be legitimate crypto-asset projects, misleading investors into purchasing tokens associated with a project, before ultimately draining the funds provided by those investors and disappearing, typically driving the token's value to zero.[116]

- *Thefts:* Of the $14 billion in crypto-asset-based crime in 2021, theft rose by over 500% year-over-year to $3.2 billion in total.[117] Thefts include security breaches that target individuals' private keys, which can be obtained through phishing, key logging, or social engineering, code exploits, and flash loan attacks.[118] 2021 also marked the first year when the level of theft in DeFi surpassed theft on centralized exchanges; out of $3.2 billion of total stolen funds, $2.3 billion was stolen from DeFi protocols, as opposed to centralized platforms, which represented a year-over-year increase of over 1,300%.[119]

  Analysts believe that most instances of theft from DeFi protocols can be traced back to errors in the smart contract code governing those protocols, which hackers exploit to steal funds, or promoters exploit flaws in their operating code that can lead to erroneous transactions, similar to the errors that allow rug pulls to occur. Users, who often lack the ability to read the code, must rely on a developer's word—offered, for example, through a protocol's white paper—that a smart contract will perform as described. Still, even auditing of the code may be insufficient to prevent theft as nearly 30% of code exploits and over 70% of flash loan attacks occurred on platforms audited within the prior year.[120] Sophisticated hacks, especially hacks perpetrated by nation state actors, have also emerged as an area of concern.[121]

- *Other*: Of the remaining $3 billion of crypto-asset-based crime in 2021, nearly $2 billion was associated with drug trafficking. Other activity can be traced to sales of stolen logins or credit cards, ransomware, malware, terrorism financing, and child abuse material.

---

116 Chainalysis, *supra* note 109, at 3, 5, 24, and 81-84. Note that the definition of rug pulls is evolving, particularly as an innovation in scamming. Another form of a rug pull would include limiting sell orders, where tokens are coded only to be bought but unable to be sold. *See* Valerio Puggioni, *Crypto rug pulls: What is a rug pull in crypto and 6 ways to spot it,* CoinTelegraph (Feb. 6, 2022), https://cointelegraph.com/explained/crypto-rug-pulls-what-is-a-rug-pull-in-crypto-and-6-ways-to-spot-it. *See also* Koinly, *Rug Pulls: Your Complete Guide,* (Mar. 31, 2022), https://koinly.io/blog/crypto-rug-pulls-guide.

117 *Id.*, at 6.

118 In an innovation unique to DeFi lending, some protocols may support "flash loans," which enable users to borrow, use, and repay crypto-assets in a single transaction that is recorded on the blockchain in the same data block. Because there is no default risk associated with flash loans, users can borrow without posting collateral and without risk of being liquidated. A "flash loan attack" can occur when the temporary surge of funds obtained in a flash loan is used to manipulate prices of crypto-assets, often through the interaction of multiple DeFi services, enabling attackers to take over the governance of a protocol, change the code, and drain the treasury. *See, e.g.*, World Economic Forum, Decentralized Finance (DeFI) Policy-Maker Toolkit 18 (2021), https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf. *See also* Shaurya Malwa, *Solana DeFi Protocol Nirvana Drained of Liquidity After Flash Loan Exploit,* CoinDesk (Jul. 28, 2022), https://www.coindesk.com/tech/2022/07/28/solana-defi-protocol-nirvana-drained-of-liquidity-after-flash-loan-exploit.

119 Chainalysis, *supra* note 109, at 70.

120 *Id.*, at 73.

121 Hacks linked to nation state actors, responsible for some of the unlawful activity discussed in this section, have advanced to become persistent threats in the crypto-asset industry. One example was in the play-to-earn crypto-asset segment of the ecosystem, where the game Axie Infinity collapsed following a $620 million hack of its Ronin Network side-chain, which was attributed to hackers affiliated with Democratic People's Republic of Korea. *See* Chainalysis, *supra* note 109, at 120. See also Aaron Schaffer, North Korean hackers linked to $260 million Axie Infinity crypto heist, The Washington Post (Apr. 14, 2022), https://www.washingtonpost.com/technology/2022/04/14/us-links-axie-crypto-heist-north-korea.